Chapter 1

Elliptic curves with additive reduction over p-adic fields

1.1 Introduction

In this chapter, we fix a prime p. If $E/\mathbb{Q}_p$ is an elliptic curve with additive reduction, and we choose a minimal Weierstrass equation over $\mathbb{Z}_p$ for it:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}_p \text{ for each } i,$$

then we denote by $E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ the open subgroup of points that reduce to a non-singular point of the reduced curve. As is well-known, this construction does not depend on the choice of minimal Weierstrass equation.

The purpose of this chapter is to investigate the structure of $E_0(\mathbb{Q}_p)$ as a topological group. We will prove the following theorem. It is slightly less general than the main result of this chapter (Theorem 1.28), but it has the advantage that its statement is more elementary.

Theorem 1.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve with additive reduction, such that it can be given by a minimal Weierstrass equation over $\mathbb{Z}_p$:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Then the group $E_0(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$, except in the following four cases:

(i) $p = 2$ *and* $a_1 + a_3 \equiv 2 \pmod 4$*;*
(ii) $p = 3$ *and* $a_2 \equiv 6 \pmod 9$*;*
(iii) $p = 5$ *and* $a_4 \equiv 10 \pmod{25}$*;*

(iv) $p = 7$ *and* $a_6 \equiv 14 \pmod{49}$.

In each of the cases (i)-(iv), $E_0(\mathbb{Q}_p)$ *is topologically isomorphic to* $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$*, where* $\mathbb{Z}/p\mathbb{Z}$ *has the discrete topology.*

The proof of Theorem 1.1 will be given in section 1.5.5. The case $p > 7$ of Theorem 1.1 was also mentioned in [38].

We will say a few words about the idea of the proof. It is a standard fact from the theory of elliptic curves over local fields [32, VII.6.3] that $E_0(\mathbb{Q}_p)$ admits a canonical filtration

$$E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset E_3(\mathbb{Q}_p) \supset \dots,$$

where for each $i \geq 1$ the quotient $E_i(\mathbb{Q}_p)/E_{i+1}(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The quotient $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ is also isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by the fact that E has additive reduction. One has a natural isomorphism of topological groups $j\colon E_2(\mathbb{Q}_p) \xrightarrow{\sim} p^2\mathbb{Z}_p$ given by the theory of formal groups. If $p > 2$, the same theory even gives a natural isomorphism $j'\colon E_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ [32, IV.6.4(b)]. These isomorphisms identify $E_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$ for all $n \geq 2$. The idea of the proof of theorem 1.1 is to start from j or j' and, by extending its domain, to build up an isomorphism between $E_0(\mathbb{Q}_p)$ and either $\mathbb{Z}_p$ or $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$.

Rather than elliptic curves over $\mathbb{Q}_p$ with additive reduction, we consider the more general case of Weierstrass curves over $\mathbb{Z}_p$ whose generic fibre is smooth and whose special fibre is a cuspidal cubic curve. This allows more general results. Theorem 1.1 is derived as a special case.

In Section 1.6, we give examples for each prime $2 \leq p \leq 7$ of an elliptic curve $E/\mathbb{Q}$ with additive reduction at p such that $E_0(\mathbb{Q}_p)$ contains a p-torsion point defined over $\mathbb{Q}$.

1.2 Preliminaries on Weierstrass curves

All proofs of facts recalled in this section can be found in [32, Ch. IV, VII].

Let K be a finite field extension of $\mathbb{Q}_p$ for some prime p, and let $v_K\colon K \to \mathbb{Z} \cup \{\infty\}$ be its normalized valuation. Let $\mathcal{O}_K$ be the ring of integers, $\mathfrak{m}_K$ its maximal ideal and k its residue field. By a Weierstrass curve over $\mathcal{O}_K$ we mean a projective curve $\mathcal{E} \subset \mathbb{P}^2_{\mathcal{O}_K}$ defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

If moreover the generic fibre $\mathcal{E}_K$ of $\mathcal{E}$ is an elliptic curve over K with $(0:1:0)$ as the origin, then we call $\mathcal{E}$ a nice Weierstrass curve. The coefficients a_i are uniquely determined by $\mathcal{E}$. The discriminant of $\mathcal{E}$, denoted $\Delta_{\mathcal{E}}$, is defined as in [32, III.1]. The curve $\mathcal{E}$ is said to be minimal if $v_K(\Delta_{\mathcal{E}})$ is minimal among $v_K(\Delta_{\mathcal{E}'})$, where $\mathcal{E}'$ ranges over the Weierstrass curves such that $\mathcal{E}'_K \cong \mathcal{E}_K$.

We will say that a Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ has good reduction when the special fibre $\mathcal{E}_k$ is smooth, multiplicative reduction when $\mathcal{E}_k$ is nodal (i.e. there are two distinct tangent directions to the singular point), and additive reduction when $\mathcal{E}_k$ is cuspidal (i.e. one tangent direction to the singular point). A non-minimal Weierstrass curve has additive reduction. The reduction type of an elliptic curve E over K is defined to be the reduction type of a minimal Weierstrass model of E over $\mathcal{O}_K$, which is a minimal Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ such that $\mathcal{E}_K \cong E$. By the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism, this is well-defined.

We have $E(K) = \mathcal{E}(K) = \mathcal{E}(\mathcal{O}_K)$ since $\mathcal{E}$ is projective. Therefore, we have a reduction map $E(K) \to \mathcal{E}(k)$ given by restricting an element of $\mathcal{E}(\mathcal{O}_K)$ to the special fibre. By $\mathcal{E}_0(K)$ we denote the subgroup $\mathcal{E}_0(K) \subset \mathcal{E}(K)$ of points reducing to a non-singular point of the special fibre $\mathcal{E}_k$. We define the subgroup $\mathcal{E}_1(K) \subset \mathcal{E}_0(K)$ as the kernel of reduction, i.e. the points that map to the identity of $\mathcal{E}(k)$ under the reduction map. A more explicit definition of $\mathcal{E}_1(K)$ is

$$\mathcal{E}_1(K) = \{(x,y) \in \mathcal{E}(K) : v_K(x) \leq -2, v_K(y) \leq -3\} \cup \{0\}. \tag{1.2}$$

More generally, one defines subgroups $\mathcal{E}_n(K) \subset \mathcal{E}_0(K)$ for $n \geq 1$ as follows:

$$\mathcal{E}_n(K) = \{(x,y) \in \mathcal{E}(K) : v_K(x) \leq -2n, v_K(y) \leq -3n\} \cup \{0\}.$$

We thus have an infinite filtration on the subgroup $\mathcal{E}_1(K)$:

$$\mathcal{E}_1(K) \supset \mathcal{E}_2(K) \supset \mathcal{E}_3(K) \supset \cdots \tag{1.3}$$

For an elliptic curve E/K and an integer $n \geq 0$, we define $E_n(K)$ to be the subgroups of $E(K)$ corresponding to $\mathcal{E}_n(K)$, where $\mathcal{E}$ is a minimal Weierstrass model of E over $\mathcal{O}_K$. The $E_n(K)$ are well-defined, again by the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism.

Proposition 1.2. *For a nice Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_p$, there is an exact sequence*

$$0 \to \mathcal{E}_1(K) \to \mathcal{E}_0(K) \to \widetilde{\mathcal{E}}_{\mathrm{sm}}(k) \to 0,$$

where $\widetilde{\mathcal{E}}_{\mathrm{sm}}$ is the complement of the singular points in the special fibre $\widetilde{\mathcal{E}}$.

Proof. This comes down to Hensel's lemma. See [32, VII.2.1]. □

For a nice Weierstrass curve $\mathcal{E}$ over $\mathcal{O}_K$, we can consider its formal group $\widehat{\mathcal{E}}$ [32, IV.1–2]. This is a one-dimensional formal group over $\mathcal{O}_K$. Giving the data of this formal group is the same as giving a power series $F = F_{\widehat{\mathcal{E}}}$ in $\mathcal{O}_K[[X, Y]]$, called the formal group law. It satisfies

$$F(X, Y) = X + Y + (\text{terms of degree} \geq 2)$$

and

$$F(F(X, Y), Z)) = F(X, F(Y, Z)).$$

For $\mathcal{E}$ as in (1.1), the first few terms of F are given by

$$\begin{aligned} F(X,Y) &= X + Y - \\ &a_1XY - a_2(X^2Y + XY^2) - 2a_3(X^3Y + XY^3) + (a_1a_2 - 3a_3)X^2Y^2 - \\ &(2a_1a_3 + 2a_4)(X^4Y + XY^4) - (a_1a_3 - a_2^2 + 4a_4)(X^3Y^2 + X^2Y^3) + \dots \end{aligned}$$

Treating the Weierstrass coefficients a_i as unknowns, we may consider F as an element of $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[X, Y]]$ called the generic formal group law. If we make $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ into a weighted ring with weight function wt, such that $\mathrm{wt}(a_i) = i$ for each i, then the coefficients of F in degree n are homogeneous of weight $n-1$ [32, IV.1.1]. For each $n \in \mathbb{Z}_{\geq 2}$, we define power series $[n]$ in $\mathcal{O}_K[[T]]$ by $[2](T) = F(T, T)$ and $[n](T) = F([n-1](T), T)$ for $n \geq 3$. Here also, we may consider each $[n]$ either as a power series in $\mathcal{O}_K[[T]]$ or as a power series in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ called the generic multiplication by n law.

Lemma 1.3. *Let $[p] = \sum_n b_n T^n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ be the generic formal multiplication by p law. Then:*

(i) $p \mid b_n$ for all n not divisible by p;
(ii) $\mathrm{wt}(b_n) = n - 1$, considering $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ as a weighted ring as above.

Proof. Part (i) is proved in [32, IV.4.4]. Part (ii) follows from [32, IV.1.1] or what was said above. □

The series $F(u, v)$ converges to an element of $\mathfrak{m}_K$ for all $u, v \in \mathfrak{m}_K$. To $\mathcal{E}$ one associates the group $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, the $\mathfrak{m}_K$-valued points of $\widehat{\mathcal{E}}$, which as a set is just $\mathfrak{m}_K$, and whose group operation $+$ is given by $u + v = F(u, v)$ for all $u, v \in \widehat{\mathcal{E}}(\mathfrak{m}_K)$. The identity element of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ is $0 \in \mathfrak{m}_K$. If $n \geq 1$ is an

integer, then by $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ we denote the subset of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ corresponding to the subset $\mathfrak{m}_K^n \subset \mathfrak{m}_K$, where $\mathfrak{m}_K^n$ is the nth power of the ideal $\mathfrak{m}_K$ of $\mathcal{O}_K$. The groups $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ are subgroups of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, and we have an infinite filtration of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$:

$$\widehat{\mathcal{E}}(\mathfrak{m}_K) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^2) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^3) \supset \cdots \tag{1.4}$$

Proposition 1.4. *The map*

$$\begin{aligned} \psi_K \colon \mathcal{E}_1(K) &\xrightarrow{\sim} \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ (x, y) &\mapsto -x/y \\ 0 &\mapsto 0 \end{aligned}$$

is an isomorphism of topological groups. Moreover, ψ_K respects the filtrations (1.3) and (1.4), i.e. it identifies the subgroups $\mathcal{E}_n(K)$ defined above with $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$.

Proof. See [32, VII.2.2]. □

It follows from the proof given in [32, VII.2.2] that there exists a power series $w \in \mathcal{O}_K[[T]]$, with the first few terms given by

$$w(T) = T^3 + a_1 T^4 + (a_1^2 + a_2)T^5 + (a_1^3 + 2a_1 a_2 + a_3)T^6 + \ldots,$$

such that the inverse to ψ_K is given by $z \mapsto (z/w(z), -1/w(z))$. Given a finite field extension $K \subset L$, we have an obvious commutative diagram

$$\begin{array}{ccc} \mathcal{E}_1(K) & \xrightarrow{\psi_K} & \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ \Big\downarrow{\scriptstyle \text{incl}} & & \Big\downarrow{\scriptstyle \text{incl}} \\ \mathcal{E}_1(L) & \xrightarrow{\psi_L} & \widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L) \end{array}$$

Here $\widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L)$ is the set of $\mathfrak{m}_L$-valued points of the formal group of $\mathcal{E}_{\mathcal{O}_L}$, the base-change of $\mathcal{E}$ to $\mathrm{Spec}(\mathcal{O}_L)$.

1.3 Extensions of topological abelian groups

In this section, we investigate the following question. Suppose that d is a non-negative integer, that A and C are finite abelian groups considered

with the discrete topology, and that B is a topological abelian group sitting in a short exact sequence

$$0 \to \mathbb{Z}_p^d \times A \to B \to C \to 0$$

where the maps are continuous, and with the second map an embedding; determine which isomorphism types of topological abelian groups are possible for B. A partial answer, sufficient for the needs of this and later chapters, is given in Proposition 1.14.

1.3.1 The profinite topology

Definition 1.5. Let G be any group. The profinite topology on G is the coarsest topology such that, for all subgroups $H \subset G$ of finite index, the quotient map $G \to G/H$ is continuous.

Proposition 1.6. *Let G be a group. A base $\mathcal{B}$ for the profinite topology on G is obtained by letting $\mathcal{B}$ be the collection of all translates of finite index subgroups of G. Alternatively, a base $\mathcal{B}$ for the profinite topology on G is given by taking a set $\{H_i\}_{i\in I}$ of finite-index subgroups of G that is final among the set of all finite-index subgroups when ordered by inclusion, and letting $\mathcal{B}$ be the collection of the translates of each H_i.*

Proof. The first assertion is clear from the definition. The second one follows since we can write every subgroup H of G as a union of translates of an element H_i of the final set of subgroups $\{H_i\}_{i\in I}$ of G. □

Lemma 1.7. *Let $G = \mathbb{Z}_p$ considered with the p-adic topology.*

(i) The open subgroups of G are the subgroups $p^k\mathbb{Z}_p$ for $k \in \mathbb{Z}_{\geq 0}$.
(ii) The p-adic topology and the profinite topology on G are the same.

Proof. Let $H \subset \mathbb{Z}_p$ be an open subgroup of G. Since G is compact, it is of finite index; let the index of H be n. We write $n = mp^k$ with m not divisible by p. Then we have $p^k\mathbb{Z}_p = n\mathbb{Z}_p \subset H$, so H contains $p^k\mathbb{Z}_p$. The image of H in $\mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}$ must have index n as well: therefore we have $n = p^k$ and $H = p^k\mathbb{Z}_p$. Conversely, it is clear that the subgroups $p^k\mathbb{Z}_p$ of G are open. This proves (i).

The proof of (i) shows that any finite index subgroup of G is of the form $p^k\mathbb{Z}_p$, and therefore open. Hence a base for the profinite topology on G is given by the $p^k\mathbb{Z}_p$ and their translates. The same is true for the p-adic topology. □

Lemma 1.8. *If G_1 and G_2 are topological groups such that their topologies coincide with the profinite topologies, then the same is true for the topological group $G_1 \times G_2$, considered with the product topology.*

Proof. Let $G = G_1 \times G_2$. A base $\mathcal{B}$ for the product topology on G is given by taking bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for the topologies on G_1 and G_2, and defining $\mathcal{B}$ to be the collection of products $U_1 \times U_2$ with $U_i \in \mathcal{B}_i$ for $i \in \{1, 2\}$.

Now we describe the profinite topology on G. Clearly, the set $\mathcal{S}$ of subgroups of the form $H_1 \times H_2$, with H_1 of finite index in G_1 and H_2 of finite index in G_2, is final among the set of all finite-index subgroups of G. By Proposition 1.6, the collection $\mathcal{B}'$ consisting of all translates of elements of $\mathcal{S}$ is a basis for the profinite topology on G. It is now clear that $\mathcal{B}$ and $\mathcal{B}'$ are the same. □

Lemma 1.9. *Let G be a topological group and let $H \subset G$ be an open subgroup of finite index. Assume that the induced topology on H is the profinite one. Then the topology on G is the profinite one.*

Proof. A base $\mathcal{B}$ for the topology on G is given by letting $\mathcal{B}$ consist of all possible translates of a base for the topology of H. If G' has finite index in G, then $G' \cap H$ has finite index in H. Conversely, clearly every finite-index subgroup H' of H is of the form $G' \cap H$ for G' of finite index in G: one can just take $G' = H'$. Subgroups of G of the form $G' \cap H$, with G' of finite index in G, are final among the set of all finite-index subgroups of G. Hence, by Proposition 1.6, if $\mathcal{B}'$ is defined as the union of all translates of subgroups of the form $G' \cap H$ of G, then $\mathcal{B}'$ gives a base for the profinite topology on G. But it is clear that $\mathcal{B}$ and $\mathcal{B}'$ are the same. □

Corollary 1.10. *Let d be a non-negative integer, and let G be a topological group containing $\mathbb{Z}_p^d$, equipped with the p-adic topology, as an open subgroup of finite index. Then G has the profinite topology.*

Proof. By Lemmas 1.7(ii) and 1.8, we have that $\mathbb{Z}_p^d$ has the profinite topology. Lemma 1.9 shows that the same is true for G. □

1.3.2 The extension problem

Lemma 1.11. *Let d be a non-negative integer and let G be $\mathbb{Z}_p^d$. Let $H \subset G$ be a subgroup of finite index. Then H is isomorphic to $\mathbb{Z}_p^d$ as a $\mathbb{Z}_p$-submodule.*

Proof. We use the properties of G as a topological group. Since H is of finite index, it contains $p^n\mathbb{Z}_p^d$ as an open subgroup for some n, and therefore it is open in G. Hence H is also closed in G, which shows that it is actually a $\mathbb{Z}_p$-submodule of G. Since H is finitely generated (since it is the kernel of the map $G \to G/H$ between finitely generated modules over a Noetherian ring) and torsion-free over the local ring $\mathbb{Z}_p$, it is a free $\mathbb{Z}_p$-module, i.e. it is isomorphic to $\mathbb{Z}_p^r$ for some non-negative integer r. Since H contains an isomorphic image of $p^n\mathbb{Z}_p^d$ as a finite-index subgroup, we must have $r = d$. □

Lemma 1.12. *Let p be a prime, d a non-negative integer, and B a finite abelian group. Let $G = \mathbb{Z}_p^d \times B$ and let $H \subset G$ be a subgroup of finite index. Then the following statements are true.*

(i) There exists a subgroup $B' \subset B$ such that H is isomorphic to $\mathbb{Z}_p^d \times B'$.

(ii) Suppose that p does not divide $\#B$. Let $\pi_1 \colon G \to \mathbb{Z}_p^d$ and $\pi_2 \colon G \to B$ be the projections to the first and second factors. Then

$$\begin{aligned} H &\to \pi_1(H) \times \pi_2(H) \\ h &\mapsto (\pi_1(h), \pi_2(h)) \end{aligned}$$

is an isomorphism.

Proof. First we prove (i). Let $\pi_1 \colon G \to \mathbb{Z}_p^d$ be the projection to the first coordinate. Since H has finite index in G, the subgroup $\pi_1(H)$ of $\mathbb{Z}_p^d$ has finite index. By Lemma 1.11, we have that $\pi_1(H)$ is isomorphic to the free $\mathbb{Z}_p$-module $\mathbb{Z}_p^d$, which implies the existence of a section $\sigma \colon \pi_1(H) \to H$ of the restricted map $\pi_1|_H : H \to \pi_1(H)$. We define a map $\pi_2' \colon H \to B$ by $h \mapsto h - \sigma(\pi_1(h)) \in \{0\} \times B$. We claim that

$$\begin{aligned} H &\to \pi_1(H) \times \pi_2'(H) \\ h &\mapsto (\pi_1(h), \pi_2'(h)) \end{aligned}$$

is an isomorphism. Indeed, injectivity is clear, and the surjectivity follows from the fact that π_2' sends an element of the form $h_1 + b$, with $h_1 \in (\sigma \circ \pi_1)(H)$ and $b \in \{0\} \times B$, to b.

To establish (ii), we claim that if p does not divide $\#B$, the map π_2' constructed above is the restriction of the projection $\pi_2 \colon G \to B$ to H. Since $\pi_2|_H$ and π_2' coincide on $\{0\} \times B$, the two maps differ by an element of $\mathrm{Hom}(\pi_1(H), B) \cong \mathrm{Hom}(\mathbb{Z}_p^d, B)$, which is zero by the assumption on B, so the claim follows. Hence $\pi_2' = \pi_2$. Since the argument from the previous paragraph showed that $(\pi_1, \pi_2') \colon H \to \pi_1(H) \times \pi_2'(H)$ is an isomorphism, we are done. □

Lemma 1.13. *Let $0 \to A \to B \xrightarrow{g} C \to 0$ be a short exact sequence of abelian groups, and let $A = A_1 \times A_2$. If we set $B_1 = B/A_2$ and $B_2 = B/A_1$, then for i equal to 1 or 2 we have short exact sequences $0 \to A_i \to B_i \to C \to 0$, and B sits inside the short exact sequence $0 \to B \to B_1 \times B_2 \to C \to 0$, where $B \to B_1 \times B_2$ is the diagonal map.*

Proof. Dividing out $0 \to A \to B \to C \to 0$ by A_i we get,

$$0 \to A_i \to B_i \to C \to 0. \tag{1.5}$$

Taking the sum over the exact sequences (1.5) for $i \in \{1, 2\}$, we get,

$$0 \to A \to B_1 \times B_2 \to C \times C \to 0,$$

with B sitting in the short exact sequence

$$\begin{aligned} 0 \to B \to B_1 \times B_2 \to C \to 0 \\ (b_1, b_2) \mapsto g(b_1) - g(b_2) \end{aligned}$$

This proves the lemma. □

With the next proposition, we answer the question posed at the start of this section. Note that, if B' is a finite abelian group, and $G = \mathbb{Z}_p^d \times B'$ for some non-negative integer d, then B' is uniquely determined by G up to isomorphism, since we have $B' \cong G_{\text{tors}}$.

Proposition 1.14. *Let A and C be finite abelian groups considered with the discrete topology. Let d be a positive integer, let B be a topological abelian group, and let*

$$0 \to \mathbb{Z}_p^d \times A \to B \to C \to 0$$

be a short exact sequence, with continuous maps and with the second map an embedding. Then the following statements are true.

- *(i) We have $B \cong \mathbb{Z}_p^d \times B'$ as topological groups, where B' is a finite abelian group carrying the discrete topology.*
- *(ii) If $A = \{0\}$, then B' is isomorphic to a subgroup of C.*
- *(iii) If $A = \{0\}$ and $C \cong \mathbb{Z}/p\mathbb{Z}$, then B' is isomorphic to $\{0\}$ or to $\mathbb{Z}/p\mathbb{Z}$.*
- *(iv) If p divides neither $\#A$ nor $\#C$, then B' fits inside a short exact sequence $0 \to A \to B' \to C \to 0$.*

Proof. We will show existence of a finite abelian group B'' such that, as a group, B can be embedded as a finite index subgroup of $\mathbb{Z}_p^d \times B''$. By Lemma 1.12, it then follows that B is isomorphic as a group to $\mathbb{Z}_p^d \times B'$ for some subgroup B' of B''. Then, since the topological groups B and $\mathbb{Z}_p^d \times B'$ both have $\mathbb{Z}_p^d$ as a finite-index open subgroup, and since they are isomorphic as groups, by Lemma 1.10 they are isomorphic as topological groups. The existence of B'' thus proves (i).

By Lemma 1.13, there exist groups B_1 and B_2 such that B sits inside a short exact sequence of abelian groups

$$0 \to B \to B_1 \times B_2 \to C \to 0 \tag{1.6}$$

and such that there are further short exact sequences

$$0 \to \mathbb{Z}_p^d \xrightarrow{i} B_1 \xrightarrow{\pi} C \to 0 \tag{1.7}$$

and

$$0 \to A \to B_2 \xrightarrow{\rho} C \to 0. \tag{1.8}$$

Since A and C are finite abelian groups and since B is abelian, we have that B_2 is finite abelian. Furthermore, we may embed B_1 in $\mathbb{Z}_p^d \times C$ by

$$\begin{aligned} f\colon B_1 &\to \mathbb{Z}_p^d \times C \\ b &\mapsto (i^{-1}(nb), \pi(b)) \end{aligned}$$

where $n = \#C$. For the image of $\mathbb{Z}_p^d \subset B_1$ we have $f(\mathbb{Z}_p^d) = n\mathbb{Z}_p^d \times \{0\}$, so $f(B_1)$ has finite index in $\mathbb{Z}_p^d \times C$. Together with (1.6), this shows that B has finite index in $\mathbb{Z}_p^d \times B_2 \times C$. We may thus take B'' to be $B_2 \times C$, which proves (i).

If $A = \{0\}$, then in addition to (1.7),

$$0 \to \mathbb{Z}_p^d \to B_1 \xrightarrow{\pi} C \to 0$$

we have that (1.8) becomes

$$0 \to 0 \to C \xrightarrow{\mathrm{id}} C \to 0.$$

By Lemma 1.13, we have that B sits inside the exact sequence

$$0 \to B \to B_1 \times C \to C \to 0$$

where the map $B_1 \times C \to C$ is given by $(b, c) \mapsto \pi(b) - c$ by Lemma 1.13. This map is split by the obvious section $c \mapsto (0, c)$; hence we have $B \cong B_1$,

which by the previous paragraph is isomorphic to a subgroup of $\mathbb{Z}_p^d \times C$. Part (ii) now follows from Lemma 1.12(i).

Assertion (iii) follows from (ii).

Now the proof of (iv). Since p does not divide $\#C$, Lemma 1.12(ii) shows that B_1 is isomorphic to $\mathbb{Z}_p^d \times C$, and that, moreover, this isomorphism can be chosen in such a way that π corresponds to the projection $\mathbb{Z}_p^d \times C \to C$ to the second factor. From (1.6), we see that B is obtained as the kernel of the surjective map

$$\mathbb{Z}_p^d \times C \times B_2 \to C$$

that sends (x, c, b) to $c - \rho(b)$ by Lemma 1.13. This map has the obvious section $c \mapsto (0, c, 0)$; hence the kernel B is isomorphic to $\mathbb{Z}_p^d \times B_2$. This proves (iv). □

Remark 1.15. By repeatedly applying Proposition 1.14, we see that if we have a finite filtration

$$\mathbb{Z}_p^d = B_n \subset B_{n-1} \subset \ldots \subset B_1$$

of topological groups, in which all quotients are finite abelian groups, then B_1 is torsion-free if and only if it is topologically isomorphic to $\mathbb{Z}_p^d$.

The following is a strengthening of Proposition 1.14 in the case $d = 1$, which will be important for us.

Corollary 1.16. *Suppose we have a short exact sequence*

$$0 \to p\mathbb{Z}_p \xrightarrow{i} X \to \mathbb{Z}/p\mathbb{Z} \to 0$$

of topological abelian groups where the second arrow is a topological embedding. Then the following statements are true.

(i) If X is topologically isomorphic to $\mathbb{Z}_p$, then $v_p(i^{-1}(px)) = 1$ for all $x \in X - i(p\mathbb{Z}_p)$, where v_p is the p-adic valuation.

(ii) If X is not topologically isomorphic to $\mathbb{Z}_p$, it is topologically isomorphic to $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$, and we have $v_p(i^{-1}(px)) > 1$ for all $x \in X - i(p\mathbb{Z}_p)$.

Proof. If X is topologically isomorphic to $\mathbb{Z}_p$, the map i is given by multiplication by some unit $\alpha \in \mathbb{Z}_p^*$ followed by the inclusion $p\mathbb{Z}_p \subset \mathbb{Z}_p$. Assertion (i) follows.

If X is not topologically isomorphic to $\mathbb{Z}_p$, then by Proposition 1.14(iii) we must have $X \cong p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$. But then if $x = (y, c)$, we have $v_p(i^{-1}(px)) = v_p(py) > 1$, proving (ii). □

Corollary 1.17. *Suppose that we have an inclusion $H \subset G$ of topological groups, that*

$$0 \to H \xrightarrow{i} G \to \mathbb{Z}/p\mathbb{Z} \to 0$$

is an exact sequence with continuous maps, with i being the inclusion of H in G and $\mathbb{Z}/p\mathbb{Z}$ carrying the discrete topology, and that H is topologically isomorphic to $\mathbb{Z}/p\mathbb{Z}$. If G is topologically isomorphic to $\mathbb{Z}_p$, then $pG = H$, and any topological isomorphism $\phi\colon H \xrightarrow{\sim} p\mathbb{Z}_p$ extends to a topological isomorphism $\widetilde{\phi}\colon G \xrightarrow{\sim} \mathbb{Z}_p$.

Proof. If G is isomorphic to $\mathbb{Z}_p$, then it follows from Corollary 1.16 that $pG = H$. Furthermore, fixing topological isomorphisms $\phi\colon H \xrightarrow{\sim} p\mathbb{Z}_p$ and $\phi'\colon G \xrightarrow{\sim} \mathbb{Z}_p$, we get a commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{\phi} & p\mathbb{Z}_p \\ \downarrow & & \vdots\, a \\ G & \xrightarrow{\phi'} & \mathbb{Z}_p \end{array}$$

where the dotted map is defined as $a = \phi^{-1} \circ i \circ \phi'$, making the diagram commute. Since a is continuous, there is $\alpha \in \mathbb{Z}_p^*$ such that for all $x \in p\mathbb{Z}_p$ we have $a(x) = \alpha x \in \mathbb{Z}_p$. Then $\widetilde{\phi} = \alpha^{-1}\phi'$ is the desired lift of ϕ. □

1.4 Weierstrass curves with additive reduction

Let K be a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}_K$ again be the ring of integers of K, with maximal ideal $\mathfrak{m}_K$ and residue field k.

In this section, we gather some general properties of nice Weierstrass curves over $\mathcal{O}_K$ with additive reduction.

Lemma 1.18. *Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. Then $\mathcal{E}$ is $\mathcal{O}_K$-isomorphic to a Weierstrass curve of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where all a_i lie in $\mathfrak{m}_K$.

Proof. We construct an automorphism $\alpha \in \mathrm{PGL}_3(\mathcal{O}_K)$ that maps $\mathcal{E}$ to a Weierstrass curve of the desired form. Consider a translation $\alpha_1 \in$

$\mathrm{PGL}_3(\mathcal{O}_K)$ moving the singular point of the special fibre $\mathcal{E}_k$ to $(0:0:1)$. The image $\mathcal{E}_1 = \alpha_1(\mathcal{E})$ is a Weierstrass curve with coefficients satisfying a_3, a_4, a_6 in $\mathfrak{m}_K$. There exists a second automorphism $\alpha_2 \in \mathrm{PGL}_3(\mathcal{O}_K)$, of the form $x' = x, y' = y + cx$, such that in the special fibre of $\alpha_2(\mathcal{E}_1)$ the unique tangent at $(0:0:1)$ is given by $y' = 0$. The Weierstrass curve $\mathcal{E}_2 = \alpha_2(\mathcal{E}_1)$ now has all its coefficients a_1, a_2, a_3, a_4, a_6 in $\mathfrak{m}_K$. One may thus take $\alpha = \alpha_2 \circ \alpha_1$. □

Suppose that $\mathcal{E}/\mathcal{O}_K$ is a nice Weierstrass curve given by (1.1), and suppose that the a_i are contained in $\mathfrak{m}_K$. In particular, $\mathcal{E}$ has additive reduction. If we let F denote the formal group law of $\mathcal{E}$, then the assumption on the a_i implies that $F(u, v)$ converges to an element of $\mathcal{O}_K$ for all $u, v \in \mathcal{O}_K$. Hence F can be seen to induce a group structure on $\mathcal{O}_K$, extending the group structure on $\widehat{\mathcal{E}}(\mathfrak{m}_K)$. The same statement holds true when we replace K by a finite field extension L.

Definition 1.19. Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve given by (1.1), and assume that the a_i are contained in $\mathfrak{m}_K$. For any finite field extension $K \subset L$, we denote by $\widehat{\mathcal{E}}(\mathcal{O}_L)$ the topological group obtained by endowing the space $\mathcal{O}_L$ with the group structure induced by F.

The following proposition will be fundamental in determining the structure of $\mathcal{E}_0(\mathbb{Q}_p)$ as a topological group for nice Weierstrass curves with additive reduction.

Proposition 1.20. *Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve given by (1.1), and assume that the a_i are contained in $\mathfrak{m}_K$.*

(i) The map $\Psi\colon \mathcal{E}_0(K) \to \widehat{\mathcal{E}}(\mathcal{O}_K)$ that sends (x, y) to $-x/y$ is an isomorphism of topological groups.

(ii) If $6e(K/\mathbb{Q}_p) < p - 1$, where e denotes the ramification degree, then $\mathcal{E}_0(K)$ is also topologically isomorphic to $\mathcal{O}_K$ equipped with the usual group structure.

Proof. Let π be a uniformizer for $\mathcal{O}_K$. Consider the field extension $L = K(\rho)$ with $\rho^6 = \pi$. Then define the Weierstrass curve $\mathcal{D}$ over $\mathcal{O}_L$ by

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x^4 x + \alpha_6,$$

where $\alpha_i = a_i/\rho^i$. There is a birational map $\phi\colon \mathcal{E} \times_{\mathcal{O}_K} \mathcal{O}_L \dashrightarrow \mathcal{D}$, given by $\phi(x, y) = (x/\rho^2, y/\rho^3)$. The birational map ϕ induces an isomorphism on generic fibres, and hence a homeomorphism between $\mathcal{E}(L)$ and $\mathcal{D}(L)$. Using

(1.2) and the fact that we have $(x, y) \in \mathcal{E}_0(L)$ if and only if $v_L(x), v_L(y)$ are both not greater than zero, one sees that ϕ induces a bijection $\mathcal{E}_0(L) \xrightarrow{\sim} \mathcal{D}_1(L)$, that all maps (*a priori* just of sets) in the following diagram are well-defined, and that the diagram commutes:

$$\begin{array}{ccccccc} \mathcal{E}_1(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(L) & \xrightarrow{\phi} & \mathcal{D}_1(L) \\ \downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi_L} & & \downarrow{\scriptstyle \psi_L} \\ \widehat{\mathcal{E}}(\mathfrak{m}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_L) & \xrightarrow{\cdot\rho} & \widehat{\mathcal{D}}(\mathfrak{m}_L) \end{array}$$

Here the map $\Psi_L \colon \mathcal{E}_0(L) \to \mathcal{O}_L$ is defined by $(x, y) \mapsto -x/y$, the rightmost lower horizontal arrow is multiplication by ρ, and the maps labeled incl are the obvious inclusions. Note that the horizontal and vertical outer maps are all continuous. Since ψ_L, ϕ and multiplication by ρ are homeomorphisms (for ψ_L one uses Proposition 1.4), so is Ψ_L. Hence Ψ must be a homeomorphism onto its image. By Galois theory, Ψ is surjective, so it is itself a homeomorphism.

Let $F_{\widehat{\mathcal{D}}}$ be the formal group law of $\mathcal{D}$. One calculates that

$$\rho F(X, Y) = F_{\widehat{\mathcal{D}}}(\rho X, \rho Y).$$

Hence all maps in the diagram are group homomorphisms. This proves the first part of the proposition.

Now assume $6e(K/\mathbb{Q}_p) < p - 1$, so that $v_L(p) = 6v_K(p) = 6e(K/\mathbb{Q}_p) < p - 1$. Now [32, IV.6.4(b)] implies that $\mathcal{E}_1(K)$ is topologically isomorphic to $\mathfrak{m}_K$, and $\mathcal{D}_1(L)$ to $\mathfrak{m}_L$. Since $\mathcal{E}$ has additive reduction, we have $\widetilde{\mathcal{E}}_{\text{sm}}(k) \cong k^+ \cong (\mathbb{Z}/p\mathbb{Z})^f$, where $f = f(K/\mathbb{Q}_p)$ is the inertia degree of $K/\mathbb{Q}_p$ and $\widetilde{\mathcal{E}}_{\text{sm}}$ is the smooth locus of the special fibre of $\mathcal{E}$. Proposition 1.2 shows we have a short exact sequence

$$0 \to \mathfrak{m}_K \to \mathcal{E}_0(K) \to (\mathbb{Z}/p\mathbb{Z})^f \to 0.$$

In the diagram above, the topological group $\mathcal{E}_0(K)$ is mapped homomorphically into the torsion-free group $\mathcal{D}_1(L)$, hence it is itself torsion-free. It follows from Remark 1.15 that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$. This proves the second part. □

The following corollary is worth noting, but will not be used in what follows.

Corollary 1.21. *Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve with additive reduction. If $6e(K/\mathbb{Q}_p) < p-1$, then $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$.*

Proof. The statement that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$ only depends on the $\mathcal{O}_K$-isomorphism class of $\mathcal{E}$. By Lemma 1.18, there exists a Weierstrass curve $\mathcal{E}'$ with $a_i \in \mathfrak{m}_K$ that is $\mathcal{O}_K$-isomorphic to $\mathcal{E}$. Now apply Proposition 1.20 to $\mathcal{E}'$. □

1.5 Proof of the main theorem

In this section, we gather some general properties of nice Weierstrass curves over $\mathbb{Z}_p$ with additive reduction and finish the proof of Theorem 1.1.

Lemma 1.22. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve with additive reduction. Then there exists a topological isomorphism $\chi\colon \widehat{\mathcal{E}}(p\mathbb{Z}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ that, for all $n \in \mathbb{Z}_{\geq 1}$, identifies $\widehat{\mathcal{E}}(p^n\mathbb{Z}_p)$ with $p^n\mathbb{Z}_p$.*

Proof. For $p > 2$, this is standard; the proof may be found in [32, IV.6.4(b)]. We now treat the case $p = 2$. By Lemma 1.18, we may assume that the Weierstrass coefficients a_i of $\mathcal{E}$ all lie in $2\mathbb{Z}_2$. The multiplication by 2 on $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ is given by the power series

$$[2](T) = F_{\widehat{\mathcal{E}}}(T,T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \dots, \qquad (1.9)$$

where $F_{\widehat{\mathcal{E}}}$ is the formal group law of $\mathcal{E}$. By [32, IV.3.2(a)], $\widehat{\mathcal{E}}(2\mathbb{Z}_2)/\widehat{\mathcal{E}}(4\mathbb{Z}_2)$ is cyclic of order 2. By [32, IV.6.4(b)], there exists a topological isomorphism $\widehat{\mathcal{E}}(4\mathbb{Z}_2) \xrightarrow{\sim} 4\mathbb{Z}_2$. Hence there exists an extension

$$0 \to 4\mathbb{Z}_2 \xrightarrow{i} \widehat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

From Proposition 1.14 we see that $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ is topologically isomorphic either to $2\mathbb{Z}_2$ or to $4\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Assume that the latter is the case, then there is an element z of order 2 in $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ that is not contained in $\widehat{\mathcal{E}}(4\mathbb{Z}_2)$. For such a z we have $v_2(z) = 1$, where $v_2\colon \widehat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}_{\geq 1} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $2\mathbb{Z}_2$ of $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$. Using that in the duplication power series (1.9) we have $a_i \in 2\mathbb{Z}_2$ for each i, it follows that $v_2([2](z)) = 2$, so $[2](z) \neq 0$. This is a contradiction, so there exists an isomorphism $\chi\colon \widehat{\mathcal{E}}(2\mathbb{Z}_2) \xrightarrow{\sim} 2\mathbb{Z}_2$ as topological groups. From this, and from the fact that $\widehat{\mathcal{E}}(2^n\mathbb{Z}_2)/\widehat{\mathcal{E}}(2^{n+1}\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \in \mathbb{Z}_{\geq 1}$ [32, IV.3.2(a)], we see that χ necessarily respects the filtrations on either side. □

Corollary 1.23. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve with additive reduction. Then there exists an isomorphism $\mathcal{E}_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ which for $n \in \mathbb{Z}_{\geq 1}$ identifies $\mathcal{E}_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$.*

Proof. Such an isomorphism can be obtained by composing the isomorphism χ from Lemma 1.22 with the isomorphism $\psi_{\mathbb{Q}_p}$ from Proposition 1.4. □

1.5.1 The case $p = 2$

Proposition 1.24. *Let $\mathcal{E}/\mathbb{Z}_2$ be a nice Weierstrass curve with its coefficients a_i in $2\mathbb{Z}_2$. Then $\mathcal{E}_0(\mathbb{Q}_2)$ is topologically isomorphic to $\mathbb{Z}_2$ if $a_1+a_3 \equiv 0 \pmod 4$, and to $2\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ otherwise.*

Proof. Proposition 1.2 shows that there is a short exact sequence

$$0 \to \mathcal{E}_1(\mathbb{Q}_2) \to \mathcal{E}_0(\mathbb{Q}_2) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

By Lemma 1.22, we have $\mathcal{E}_1(\mathbb{Q}_2) \cong 2\mathbb{Z}_2$, so Proposition 1.14 implies that $\mathcal{E}_0(\mathbb{Q}_2)$ is topologically isomorphic either to $\mathbb{Z}_2$ or to $2\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Let $[2](T) \in \mathcal{O}_K[[T]]$ be the formal duplication formula (1.9) on $\mathcal{E}$. Let Ψ be the map from Proposition 1.20. Since Ψ is an isomorphism of topological groups, we have for all $P \in \mathcal{E}_0(\mathbb{Q}_2)$:

$$\Psi(2P) = [2](\Psi(P)). \tag{1.10}$$

By Corollary 1.16, we have $\mathcal{E}_0(\mathbb{Q}_2) \cong \mathbb{Z}_2$ if and only if for all $P \in \mathcal{E}_0(\mathbb{Q}_2) - \mathcal{E}_1(\mathbb{Q}_2)$ we have $2P \in \mathcal{E}_1(\mathbb{Q}_2) - \mathcal{E}_2(\mathbb{Q}_2)$, which by (1.10) is true if and only if for all $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$ we have $v_2([2](z)) = 1$, where $v_2\colon \widehat{\mathcal{E}}(\mathbb{Z}_2) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $\mathbb{Z}_2$ of $\widehat{\mathcal{E}}(\mathbb{Z}_2)$. This condition may be checked using the duplication power series

$$[2](T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \ldots = \sum_{i=1}^{\infty} b_iT^i.$$

In deciding whether $v_2([2](z)) = 1$ for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$, we do not need to consider those parts of terms whose coefficients have valuation ≥ 2. The non-linear parts of each coefficient b_i will contribute only terms with valuation ≥ 2, so may ignore these and keep only the linear parts. The terms b_iz^i with i odd and greater than 1 we may discard altogether; by Lemma 1.3, all their coefficients have valuation ≥ 2. Finally, we may discard all terms b_iz^i with i even and ≥ 6: a polynomial in $\mathbb{Z}[a_1, \ldots, a_6]$ whose weight

is odd and at least 5 does not contain a linear term (there being no a_5), so the terms involving $z^6, z^8, z^{10}, \ldots$ will have valuation ≥ 2.

We thus get that, if $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$,

$$v_2([2](z)) = 1 \quad \Leftrightarrow \quad v_2(2z - a_1 z^2 - 7a_3 z^4) = 1.$$

The last statement is true for all $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$ if and only if

$$v_2\left(z - \frac{a_1}{2}z^2 - \frac{7a_3}{2}z^4\right) = 0 \Leftrightarrow a_1 + 7a_3 \equiv 0 \bmod 4 \Leftrightarrow a_1 + a_3 \equiv 0 \bmod 4$$

since $z \equiv z^2 \equiv z^4 \pmod 2$. This proves the proposition. □

1.5.2 The case $p = 3$

Proposition 1.25. *Let $\mathcal{E}/\mathbb{Z}_3$ be a nice Weierstrass curve with its coefficients a_i in $3\mathbb{Z}_3$. Then $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if $a_2 \not\equiv 6 \pmod 9$, and to $3\mathbb{Z}_3 \times \mathbb{Z}/3\mathbb{Z}$ otherwise.*

Proof. We proceed as in the proof of Proposition 1.24, using the formal triplication formula:

$$[3](T) = 3T - 3a_1T^2 + (a_1^2 - 8a_2)T^3 + (12a_1a_2 - 39a_3)T^4 + \ldots = \sum_{i=1}^{\infty} b_i T^i. \tag{1.11}$$

We consider the usual exact sequence for $\mathcal{E}_0(\mathbb{Q}_3)$:

$$0 \to \mathcal{E}_1(\mathbb{Q}_3) \to \mathcal{E}_0(\mathbb{Q}_3) \to \mathbb{Z}/3\mathbb{Z} \to 0.$$

We see from $\mathcal{E}_1(\mathbb{Q}_3) \cong 3\mathbb{Z}_3$ and Corollary 1.16 that $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $3\mathbb{Z}_3 \times \mathbb{Z}/3\mathbb{Z}$ if and only if for all elements $z \in \widehat{\mathcal{E}}(\mathbb{Z}_3) - \widehat{\mathcal{E}}(3\mathbb{Z}_3)$, $[3](z)$ has valuation greater than 1. On the other hand, $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if for all such z, the valuation of $[3](z)$ is 1. Reasoning as in the proof of Proposition 1.24, we see that we may ignore all terms whose degree is not 1 and not a multiple of 3, since these have coefficients divisible by 3 and of positive weight. Also we may ignore the terms of degree both equal to a multiple of 3 and greater than 3, since their coefficients do not contain parts that are linear in $a_1, \ldots, a_6$. Finally, we may ignore the non-linear part of the term of degree 3. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_3) - \widehat{\mathcal{E}}(3\mathbb{Z}_3)$, we have

$$v_3([3](z)) = 1 \quad \Leftrightarrow \quad v_3(3z - 8a_2z^3) = 1.$$

The last statement is true for all such z if and only if

$$v_3\left(z - \frac{8a_2}{3}z^3\right) = 0 \Leftrightarrow 1 - \frac{8a_2}{3} \not\equiv 0 \bmod 3 \Leftrightarrow a_2 \not\equiv 6 \bmod 9$$

since $z \equiv z^3 \pmod 3$. This proves the proposition. □

1.5.3 The case $p = 5$

Proposition 1.26. *Let $\mathcal{E}/\mathbb{Z}_5$ be a nice Weierstrass curve with its coefficients a_i in $5\mathbb{Z}_5$. Then $\mathcal{E}_0(\mathbb{Q}_5)$ is topologically isomorphic to $\mathbb{Z}_5$ if $a_4 \not\equiv 10 \pmod{25}$, and to $5\mathbb{Z}_5 \times \mathbb{Z}/5\mathbb{Z}$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 5 power series in the case where a_1, a_2, a_3 are zero:

$$[5](T) = 5T - 1248a_4T^5 + \ldots = \sum_{i=1}^{\infty} b_iT^i \tag{1.12}$$

This formula suffices for our purposes, since the same arguments as in the proofs of Propositions 1.24 and 1.25 show that the terms that are canceled by setting $a_1 = a_2 = a_3 = 0$ could have been ignored anyway.

We apply Corollary 1.16 to:

$$0 \to 5\mathbb{Z}_5 \to \mathcal{E}_0(\mathbb{Q}_5) \to \mathbb{Z}/5\mathbb{Z} \to 0.$$

In (1.12) we may ignore terms of degree not equal to 1 or 5, by the same reasoning as in the proofs of Propositions 1.24 and 1.25. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_5) - \widehat{\mathcal{E}}(5\mathbb{Z}_5)$ we have

$$v_5([5](z)) = 1 \quad \Leftrightarrow \quad v_5(5z - 1248a_4z^5) = 1.$$

The last statement is true for all such z if and only if

$$v_5\left(z - \frac{1248a_4}{5}z^5\right) = 0 \Leftrightarrow 1 - \frac{1248a_4}{5} \not\equiv 0 \bmod 5 \Leftrightarrow a_4 \not\equiv 10 \bmod 25$$

since $z \equiv z^5 \pmod 5$. This proves the proposition. □

1.5.4 The case $p = 7$

Proposition 1.27. *Let $\mathcal{E}/\mathbb{Z}_7$ be a nice Weierstrass curve with its coefficients a_i in $7\mathbb{Z}_7$. Then $\mathcal{E}_0(\mathbb{Q}_7)$ is topologically isomorphic to $\mathbb{Z}_7$ if $a_6 \not\equiv 14 \pmod{49}$, and to $7\mathbb{Z}_7 \times \mathbb{Z}/7\mathbb{Z}$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 7 power series with a_1, a_2, a_3 set to zero:

$$[7](T) = 7T - 6720a_4T^5 - 352944a_6T^7 + \dots \tag{1.13}$$

As before, the terms that have disappeared as a result could have been ignored anyway.

We apply Corollary 1.16 to:

$$0 \to 7\mathbb{Z}_7 \to \mathcal{E}_0(\mathbb{Q}_7) \to \mathbb{Z}/7\mathbb{Z} \to 0,$$

In (1.13) we may ignore terms of degree not equal to 1 or 7, by the same reasoning as in the proofs of Propositions 1.24 and 1.25. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_7) - \widehat{\mathcal{E}}(7\mathbb{Z}_7)$ we have

$$v_7([7](z)) = 1 \quad \Leftrightarrow \quad v_7(7z - 352944a_6z^7) = 1.$$

The last statement is true for all such z if and only if

$$v_7\left(z - \frac{352944a_6}{7}z^7\right) = 0 \Leftrightarrow 1 - \frac{352944a_6}{7} \not\equiv 0 \bmod 7 \Leftrightarrow a_6 \not\equiv 14 \bmod 49$$

since $z \equiv z^7 \pmod 7$. This proves the proposition. □

1.5.5 The proof

We are now ready to derive Theorem 1.1 from our previous results. In fact, we state a more general version of that theorem, since it is also valid for non-minimal Weierstrass equations.

Theorem 1.28. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve given by*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Then there is a topological isomorphism between $\mathcal{E}_0(\mathbb{Q}_p)$ and $\mathbb{Z}_p$, except in the following four cases:

(i) $p = 2$ *and* $a_1 + a_3 \equiv 2 \pmod 4$*;*
(ii) $p = 3$ *and* $a_2 \equiv 6 \pmod 9$*;*
(iii) $p = 5$ *and* $a_4 \equiv 10 \pmod{25}$*;*
(iv) $p = 7$ *and* $a_6 \equiv 14 \pmod{49}$*.*

Moreover, every isomorphism between $\mathcal{E}_0(\mathbb{Q}_p)$ *and* $\mathbb{Z}_p$ *identifies* $\mathcal{E}_n(\mathbb{Q}_p)$ *with* $p^n\mathbb{Z}_p$ *for all* $n \in \mathbb{Z}_{\geq 0}$*. In each of the cases (i)-(iv),* $\mathcal{E}_0(\mathbb{Q}_p)$ *is topologically isomorphic to* $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$*, where* $\mathbb{Z}/p\mathbb{Z}$ *has the discrete topology.*

Proof. The isomorphism type of $\mathcal{E}_0(\mathbb{Q}_p)$ follows from applying part (ii) of Proposition 1.20 if $p > 7$, or one of Propositions 1.24–1.27 if $p \leq 7$.

We claim that, if $\mathcal{E}_0(\mathbb{Q}_p) \cong \mathbb{Z}_p$, then the isomorphism can be chosen in such a way that $\mathcal{E}_n(\mathbb{Q}_p)$ is identified with $p^n\mathbb{Z}_p$ for all $n \in \mathbb{Z}_{\geq 0}$. For this, we choose the topological isomorphism $\chi\colon \mathcal{E}_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ from Lemma 1.22. By Corollary 1.17, the map χ extends to a topological isomorphism

$$\widetilde{\chi}\colon \mathcal{E}_0(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p$$

and we have $p\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}_1(\mathbb{Q}_p)$. It follows from Lemma 1.22 that $p^n\mathcal{E}_0(\mathbb{Q}_p)$ equals $\mathcal{E}_n(\mathbb{Q}_p)$; hence *every* group isomorphism $\mathcal{E}_0(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p$ will identify $\mathcal{E}_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$. This concludes the proof. □

Proof of Theorem 1.1. Theorem 1.1 follows by applying Theorem 1.28 to a minimal Weierstrass equation of E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Such an equation exists by Lemma 1.18. □

1.6 Examples

In this section, we have collected some examples of elliptic curves over $\mathbb{Q}_p$ with additive reduction, such that their points of good reduction contains a p-torsion point. All curves and torsion points in these examples are defined over $\mathbb{Q}$. The fact that they possess a p-torsion point of good reduction can be verified using the appropriate result from the previous section.

Example 1.29. The elliptic curve

$$E_2\colon y^2 - 2y = x^3 - 2$$

has additive reduction at 2, and its 2-torsion point $(1, 1)$ is of good reduction.

Example 1.30. The elliptic curve

$$E_3 \colon y^2 = x^3 - 3x^2 + 3x$$

has additive reduction at 3, and its 3-torsion point $(1, 1)$ is of good reduction.

Example 1.31. The elliptic curve

$$E_5 \colon y^2 - 5y = x^3 + 20x^2 - 15x$$

has additive reduction at 5, and its 5-torsion point $(1, -1)$ is of good reduction.

Example 1.32. The elliptic curve

$$E_7 \colon y^2 + 7xy - 28y = x^3 + 7x - 35$$

has additive reduction at 7, and its 7-torsion point $(2, 1)$ is of good reduction.